Amendments to the Claims

1. (Currently amended) A branding process to establish a trust web of networked computing devices on an open multi-access network, comprising:

securely networking a security-uninitialized device with a branding device via a secured network medium;

~~electronically imprinting the security-uninitialized device with~~ generating group membership and cryptographic key data ~~by~~ at the branding device ~~via the secured network medium~~, the cryptographic key data for verifying group membership information provided by other devices on the open multi-access network to the security-uninitialized device are authenticated by the branding device

electronically imprinting the security-uninitialized device with the group membership and cryptographic key data by transmitting the group membership and cryptographic key data from the branding device to the security-uninitialized device via the secured network medium; and

initializing the security-uninitialized device to use the cryptographic key data to authenticate group membership of other devices interacting with the security-uninitialized device on the open multi-access network, and to provide the security-uninitialized device's group membership to such other devices as authentication that the security-uninitialized device is a member of the trust web, such that at least some interaction via the open multi-access network with the security-uninitialized device is cryptographically secured to only other devices in the trust web.

2. (Currently amended) A branding process to establish cryptographically secured interaction among networked computing devices within a trust group, the trust group comprising a group of devices, on an open multi-access network, comprising:

securely networking a security-uninitialized device with a branding device via a secured network medium;

~~transmitting~~ generating a branding certificate ~~from~~ at the branding device ~~to the security-uninitialized device via the secured network medium~~, the branding certificate instructing that the security-uninitialized device trust the branding device, the branding certificate further containing key data for verifying certificates provided by other devices on the open multi-access network to the security-uninitialized device are authenticated by the branding device;

transmitting the branding certificate from the branding device to the security-uninitialized device via the secured network medium;

~~transmitting~~ generating a trust group membership certificate at the branding device which is signed by the branding device ~~to the security-uninitialized device via the secured network medium~~, the trust group membership certificate containing a signed group name as well as a signed key identifying the security-uninitialized device such that, when the security-uninitialized device sends the trust group certificate to a branded device which is a member of the trust group, the trust group certificate is validated by the branded device, and the branded device verifies that the security-uninitialized device identified in the trust group membership certificate is a member of the trust group of devices referred to by the group name;

transmitting the trust group membership certificate from the branding device to the security-uninitialized device via the secured network medium; and

initializing a security resolver of the security-uninitialized device to use the key data of the branding certificate to authenticate other devices interacting with the security-uninitialized device on the open multi-access network are in the trust group, and to provide the trust group membership certificate to such other devices as authentication that the security-uninitialized device is a member of the trust group, such that at least some interaction via the open multi-access network with the security-uninitialized device is cryptographically secured to only other devices in the trust group.

3. (Original) The branding process of claim 2 wherein securely networking the security-uninitialized and branding devices comprises networking the devices via a limited access network interface of the security-uninitialized device that is separate from the security-uninitialized device's interface to the open multi-access network.

4. (Original) The branding process of claim 3 wherein the limited access network interface is of a direct device-to-device wired networking medium.

5. (Original) The branding process of claim 3 wherein the limited access network interface is of a directional wireless networking medium.

6. (Original) The branding process of claim 2 wherein securely networking the security-uninitialized and branding devices comprises:

placing transmitter/receivers of the security-uninitialized and branding devices for an omni-directional wireless networking medium into a wave guide and/or Faraday cage; and

networking the devices with the wave guide and/or Faraday cage via the omni-directional wireless networking medium.

7. (Original) The branding process of claim 2 further comprising:

transmitting a principal identifier from the branding device to the security-uninitialized device, the principal identifier providing a cryptographically secured identity to the security-uninitialized device, the principal identifier containing a public/private key pair; and

using the public/private key pair to encrypt interaction of the security-uninitialized device with said other devices authenticated to be in the trust group.

8. (Original) The branding process of claim 7 wherein the principal identifier further contains a name for the security-uninitialized device, the process further comprising identifying the security-uninitialized device to human operators using the name.

9. (Original) The branding process of claim 8 further comprising prompting a human user of the branding device to enter the name upon performing the branding process on the security-uninitialized device.

10. (Original) The branding process of claim 2 further comprising initially distributing the security-uninitialized device in a retail channel prior to having the branding process performed on the security-uninitialized device.

11. (Original) The branding process of claim 10 further comprising upon completion of initializing the security resolver, disallowing the security-uninitialized device from having the branding process again performed on the security-uninitialized device until the now initialized security of the security-unitialized device is reset.

12. (Original) The branding process of claim 10 further comprising upon completion of initializing the security resolver, allowing the branding process to be performed only via a limited access network interface of the security-uninitialized device.

13. (Currently amended) A networked computing device supporting branding to establish cryptographically secured interaction with other devices within a trust group of devices on an open-access network, the networked computing device comprising:

a network interface for communicating on the open-access network;

a security resolver operational after being initialized with a branding public key to authenticate trust group membership certificates separate from the branding public key provided to the networked computing device from other devices via the network interface using the branding public key, and further operational to inhibit interaction via the network interface with other devices not authenticated as in the trust group of devices, the security resolver being initially uninitialized; and

a security initializer operational to receive the branding public key from a branding device securely networked to the networked computing device, the branding device having previously generated the branding public key and trust group membership certificates, and further operational to initialize the security resolver with the branding public key.

14. (Original) The networked computing device of claim 13 further comprising:

a limited access networking interface; and

the security initializer further operational to accept the branding public key when received from the branding device only via the limited access networking interface.

15. (Original) The networked computing device of claim 13 further comprising:

the security initializer further operational to accept the branding public key when received from the branding device via the network interface when in an initial unbranded state; and

a branding reset operational upon activation to return the security initializer to the initial unbranded state.

16. (Original) The networked computing device of claim 13 further comprising:

a branding mode activator operational to place the networked computing device in a branding mode; and

the security initializer further operational to accept the branding public key when received from the branding device via the network interface when in the branding mode.

17. (Original) The networked computing device of claim 13 further comprising:

the security resolver further operational when initialized with a trust group membership certificate to provide the trust group membership certificate to other devices via the network interface to attest to membership of the networked computing in the trust group; and

the security initializer further operational to receive the trust group membership certificate from the branding device while securely networked to the networked computing device, and further operational to initialize the security resolver with the trust group membership certificate.

18. (Original) The networked computing device of claim 13 further comprising:

the security resolver further operational when initialized with a public/private key pair to encrypt interaction via the network interface with other devices authenticated as in the trust group using the public/private key pair; and

the security initializer further operational to receive the public/private key pair from the branding device while securely networked to the networked computing device, and further operational to initialize the security resolver with the public/private key pair.

19. (Currently amended) The branding process of claim 1, wherein the group membership information comprises a certificate signed and generated by the branding device and containing a signed group name as well as signed information naming the security-uninitialized device such that, when the security-uninitialized device provides the certificate to a branded device which is a member of the trust web, the certificate is validated by the branded device, and the branded device verifies that the security-uninitialized device named in the certificate is a member of the trust group of devices referred to by the group name.

20. (Previously presented) The networked computing device of claim 13, wherein:

each trust group membership certificate is sent by an other device and each trust group membership certificates comprises:

a signed name for a trust group; and

a signed identifier for the other device sending the trust group membership certificate; and

the security resolver is configured to authenticate trust group membership certificates by:

authenticating, from the trust group membership certificate, the signed name for the trust group and the signed identifier for the other device sending the trust group membership certificate using the branding public key; and

when the signed name for a trust group matches the trust group, verifying that the other device sending the trust group membership certificate is a member of the trust group.